

WE CLAIM:

1. A network device for managing a communication over a network, comprising:
 - a transceiver arranged to send and to receive the communication over the network;
 - a processor, coupled to the transceiver, that is configured to perform actions, including:
 - receiving a proxy request from a client through a secure tunnel;
 - modifying the proxy request to include a security attribute; and
 - forwarding the modified proxy request to a proxy service,wherein the security attribute enables a proxy connection through the secure tunnel.
2. The network device of Claim 1, wherein modifying the proxy request further comprises including a security header with the proxy request.
3. The network device of Claim 1, wherein the security attribute further comprises at least one of an IP address associated with the client, a security property associated with the secure tunnel, a public key certificate, a security credential associated with the client, access control data configured to enable the client access to a content server, a session identifier, and an identifier associated with the secure tunnel.
4. The network device of Claim 1, wherein the proxy request is an HTTP proxy request.
5. The network device of Claim 1, wherein the secure tunnel further comprises at least one of an SSL tunnel, a TLS tunnel, HTTP Secure (HTTPS), Tunneling TLS (TTLS), and an EAP secure tunnel.

6. The network device of Claim 1, further comprising receiving an HTTPS communication to enable the secure tunnel.

7. An apparatus for managing a communication over a network, comprising:

a transceiver arranged to send and to receive the communication over the network;

a processor, coupled to the transceiver, that is configured to perform actions, including:

establishing a secure tunnel between the apparatus and a client;
receiving a proxy request from the client through the secure

tunnel;

modifying the proxy request to include a security attribute; and
forwarding the modified proxy request to a proxy service,

wherein the security attribute enables a proxy connection through the secure tunnel.

8. The apparatus of Claim 7, wherein establishing the secure tunnel further comprises receiving an HTTPS communication.

9. The apparatus of Claim 7, wherein the apparatus is operable as at least one of a firewall, a gateway, and a proxy server.

10. A method for managing a communication over a network, comprising:
receiving a proxy request from a client through a secure tunnel;
modifying the proxy request to include a security attribute; and
forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

11. The method of Claim 10, wherein modifying the proxy request further comprises associating a security header with the proxy request.

{S:\8212\0200359-us0\80002594.DOC [REDACTED] }

12. The method of Claim 10, wherein the security attribute further comprises at least one of an IP address associated with the client, a security property associated with the secure tunnel, a public key certificate, access control data configured to enable the client access to a content server, a security credential associated with the client, a session identifier, and an identifier.

13. The method of Claim 10, wherein the proxy request is an HTTP proxy request.

14. The method of Claim 10, wherein the secure tunnel further comprises at least one of an SSL tunnel, a TLS tunnel, HTTP Secure (HTTPS), Tunneling TLS (TTLS), IPSec tunnel, and an EAP secure tunnel.

15. The method of Claim 10, further comprising receiving an HTTPS communication to enable the establishment of the secure tunnel.

16. The method of Claim 10, further comprising:
initiating a connection to a secure tunnel client; and
sending the proxy request to the secure tunnel client, wherein the secure tunnel client is configured to forward the proxy request over the secure tunnel.

17. The method of Claim 10, wherein modifying the proxy request further comprises modifying the proxy request employing an access control service.

18. A system for managing a communication over a network, comprising:
a client that is configured to perform actions, including:
determining a secure tunnel; and
sending a proxy request through the determined secure tunnel;
and

a server, coupled to the client, that is configured to perform actions,
including:

receiving the proxy request from the client through the secure
tunnel;

modifying the proxy request to include a security attribute; and
forwarding the modified proxy request to a proxy service,
wherein the security attribute enables a proxy connection through the secure tunnel.

19. The system of Claim 18, wherein the client further comprises:
a proxy client that is configured to generate a proxy request; and
a secure tunnel client, coupled to the proxy client, that is configured to
establish the secure tunnel with the server.


20. The system of Claim 19, wherein the proxy client further comprises a
port-forwarding client application.

21. The system of Claim 18, wherein modifying the proxy request further
comprises including a security header with the proxy request.

22. The system of Claim 18, wherein the security attribute further comprises
at least one of an IP address associated with the client, a security property associated
with the secure tunnel, a public key certificate, access control data configured to enable
the client access to a content server, a security credential associated with the client, a
session identifier, and an identifier associated with the secure tunnel.

23. The system of Claim 18, wherein the proxy request is an HTTP proxy
request.

24. The system of Claim 18, wherein the secure tunnel further comprises a
means for securing the communication over the network.

{S:\8212\0200359-us0\80002594.DOC  }

25. The system of Claim 18, wherein the secure tunnel further comprises at least one of an SSL tunnel, a TLS tunnel, HTTP Secure (HTTPS), Tunneling TLS (TTLS), IPSec tunnel, and an EAP secure tunnel.

26. The system of Claim 18, wherein determining the secure tunnel further comprises generating an HTTPS message to enable the secure tunnel.

27. An apparatus for managing a communication over a network, comprising:
a transceiver arranged to send and to receive the communication over the network;
a processor, coupled to the transceiver, that is configured to receive a proxy request from a client through a secure tunnel;
a means for modifying the proxy request to include a security attribute;
and
a means for forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

28. The apparatus of Claim 27, wherein the secure tunnel further comprises a means for securing the communication over the network.